

Hauptstudium

I – Funktionentheorie

1. Differenzierbarkeit im \mathbb{R}^n und im Komplexen

Definition der Differenzierbarkeit in mehreren Veränderlichen (partielle Ableitungen), Def. von total differenzierbar. **Hinreichend** für totale Differenzierbarkeit ist die Stetigkeit der partiellen Ableitungen. Partielle Ableitungen von Beispielen berechnen. Def. der komplexen Zahlen. Def. von \exp , \sin , \cos durch auf ganz \mathbb{C} konvergente Potenzreihen. Eulersche Formeln. Ist \cos , \sin im Komplexen beschränkt? Was ist $|\exp(z)|$ für $z \in \mathbb{C}$? Polarkoordinaten $z = r \exp(i\varphi)$. Damit kann man Multiplikation, Wurzelziehen etc. geometrisch deuten! Weshalb ist \exp im Komplexen periodisch? Weshalb ist $\exp : \mathbb{C} \rightarrow \mathbb{C}^*$ surjektiv? (Schreibe $w = r \exp(i\varphi)$. Dann ist bei $z := \log r + i\varphi + 2k\pi i$ für $k \in \mathbb{Z}$ stets $\exp z = w$.) Def. der nicht eindeutigen “Funktion” $z = \log w$ durch obige Formel. Wird willkürlich $-\pi < \operatorname{Im} z \leq \pi$ vorgeschrieben, so ist $\log w$ eindeutig (“Hauptwert von $\log w$ ”).

Def. Differenzierbarkeit im Komplexen, Zusammenhang mit reell differenzierbar und Cauchy-Riemann. (Beweisidee: Komplex differenzierbar \iff approximierbar durch \mathbb{C} -lineare Funktion, reell differenzierbar \iff approximierbar durch \mathbb{R} -lineare Abbildung. Diese ist genau dann \mathbb{C} -linear, wenn C-R DGL gelten) Äquivalente Formulierung mit $\partial f / \partial \bar{z}$. (Was ist das? Warum ist das äquivalent?) Def. holomorph in z_0 (ist nicht dasselbe wie in z_0 komplex differenzierbar!). Def. holomorph in Gebiet G (dazu exakte Def. von “offen” und “zusammenhängend”). Kann eine in G holomorphe nichtkonstante Funktion nur reelle Werte annehmen? (Denk an “Cauchy-Riemann” oder “Gebietstreue”!) Im Komplexen ist (im Gegensatz zum Reellen!) eine holomorphe Funktion ∞ oft differenzierbar (weshalb? Beweisidee: Cauchy-Integralsatz \implies Integralformel \implies Potenzreihe entwickelbar $\implies \infty$ oft differenzierbar. Beweise ausführen können!)

Def. kompakte Konvergenz (deshalb wichtig, weil die meisten Reihen nicht überall gleichmäßig konvergieren, sondern nur auf jedem Kompaktum! Def. kompakt?). Vertauschungssätze (Summe und Integration) (Summe und Differentiation im **Komplexen**, nicht jedoch im Reellen!) gelten auch bei kompakter Konvergenz. Weshalb ist also $(\exp z)' = \exp z$? Es folgt, daß eine kompakt konvergente Reihe holomorpher Funktionen wieder holomorph ist (Satz von Weierstraß).

2. Kurvenintegrale im Komplexen

Definition des Kurvenintegrals im Komplexen. Berechnung $\int z^n dz$ über Kreis. Cauchy-Integralsatz (ungefähre Beweisidee?). Damit Cauchy-Integralformel (Beweisidee!). Welche Eigenschaften komplexdifferenzierbarer Funktionen folgen aus der Cauchy-Integralformel? [Analytizität, Cauchy-Ungleichungen, daraus Satz von Liouville] (Beweisideen!). Was geschieht mit dem Kurvenintegral, wenn die Funktion bis auf isolierte Stellen holomorph ist? (Residuensatz! Welche praktische Bedeutung hat dieser für reelle Integrale?) Weitere Folgerungen aus Cauchy-Integralsatz: Gebietstreue, Maximum- und Minimumprinzip. Wie folgt Minimumprinzip aus Maximumprinzip? Def. Stammfunktion. f hat Stammfunktion \iff Kurvenintegral ist wegunabhängig (Beweisidee $F(z) := \int_K f(\zeta) d\zeta$, wobei K eine Kurve von z_0 bis z ist. Wohldefiniertheit?!). Ist G einfach zusammenhängend (was ist das?), so gilt: f hat Stammfunktion $\iff f$ holomorph (Beweisidee: “ \Leftarrow ” liefert Cauchy-Integralsatz für einfach zusammenhängende G . “ \Rightarrow ” folgt wie?). Beispiel, daß nicht stets eine Stammfunktion existiert ($G = \mathbb{C}^*$, $f(z) = 1/z$). Aber $1/z$ hat auf $(\mathbb{C}^* - \mathbb{R}_{(-)})$ eine Stammfunktion (weshalb?). Wenn dies gezeigt ist, kann damit der \log definiert werden!

3. Potenzreihendarstellung

Wie können die Koeffizienten a_v der Potenzreihe $f(x) = \sum a_v (x - x_0)^v$ berechnet werden? (Antwort: $a_v = f^{(v)}(x_0)/v!$.) Def. Konvergenzradius R . Weshalb für $|z - z_0| < R$ Konvergenz, für $|z - z_0| > R$ Divergenz? (Es ist nicht klar, daß Konvergenzmenge Kreis ist!) Wie ist das Konvergenzverhalten auf dem Rand des Konvergenzradius? (Antwort: Unbestimmt). Berechnen des Konvergenzradius mit Hadamardscher Formel oder über $R = \lim \frac{a_n}{a_{n+1}}$. Eine Potenzreihe konvergiert i.a. **nicht**

gleichmäßig für alle z auf $|z - z_0| < R$, sondern nur für alle z mit $|z - z_0| \leq r$ bei festem $r < R$ (kompakte Konvergenz, s.o.!).

Im Reellen kann man es der Funktion nicht ansehen, wie groß Konvergenzradius R ist (z.B. $f(x) = 1/(1+x^2)$; $x_0 = 1$); dagegen sieht man das leicht im Komplexen: Abstand zur nächsten Singularität! (Weshalb? Das zeigt der Beweis, in dem Cauchy-Kern in geometrische Reihe entwickelt wird!) Damit folgt, daß im obigen Beispiel $R = \sqrt{2}$ ist. Wie groß ist R bei $f(z) = z/(\exp z - 1)$, um $z_0 = 0$ entwickelt?

4. IDENTITÄTSSATZ, NULLSTELLEN, SINGULARITÄTEN

Aussage Identitätssatz (beim Beweis ging entscheidend die Potenzreihenentwicklung ein). Mach Dir klar, daß äquivalent zum Identitätssatz die Aussage "jedes f hat nur isolierte Nullstellen" ist. Def. der Nullstellen- bzw. Polstellenordnung als diejenige Zahl k mit " $f(z)/(z-a)^k$ ist holomorph und ohne Nullstelle". Weshalb ist dazu äquivalent " $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0, f^{(k)}(a) \neq 0$? Was weiß man über die Nullstellenordnungen von $f+g, f \cdot g$? Wie kann man die Anzahl der Nullstellen mit Vielfachheiten durch ein Integral berechnen (Beweisidee?) Aus nullstellenzählendem Integral folgt Satz von Rouché.

Laurententwicklungen für Funktionen auf Kreisringen. Def. Residuum als a_{-1} und als $\int f(z)dz$. (Weshalb stimmen beide Def. überein? Das liegt daran, daß $(z-z_0)^n$ für $n \neq -1$ stets Stammfunktion hat!) Def. der 3 Arten von Singularitäten über Laurentreihen. Beispiele für alle 3 Arten! Wie sieht das Wachstumsverhalten in $U(z_0) - \{z_0\}$ aus? (hebbar \iff beschränkt; Pol $\iff |f(z)| \rightarrow \infty$; wesentlich \iff Casorati-Weierstraß). Mach Dir klar, daß Hebbarkeitssatz im Reellen falsch ist (Sprungfunktionen!)

5. Funktionentheoretischer Beweis des Fundamentalsatzes der Algebra

Beweis mit Liouville: Hätte das Polynom P keine Nullstelle, so wäre $1/P$ eine in ganz \mathbb{C} holomorphe Funktion. Nun ist bei **Polynom** P für $|z| \geq K$ (wobei K eine von P abhängende Konstante ist) sicher $|P(z)| \geq 1$, also $|1/P(z)| \leq 1$. Weshalb ist aber $|1/P(z)|$ beschränkt für $|z| \leq K$? Mit Liouville folgt Behauptung. Weitere Beweise mit Minimumprinzip, Rouché.

ANHANG. Besonderheiten komplexer Analysis zur reellen Analysis

Maximumprinzip, Minimumprinzip, Satz von Liouville auch für überall konvergente Potenzreihen im Reellen falsch. (Gegenbeispiel $f(z) = \sin z$!) Ferner ist eine einmal differenzierbare Funktion nicht unbedingt ∞ -oft differenzierbar; und eine ∞ -oft differenzierbare Funktion ist nicht unbedingt lokal in eine Potenzreihe entwickelbar. Umgekehrt haben im Reellen stetige Funktionen eine Stammfunktion, im Komplexen dagegen nur holomorphe Funktionen (und auch diese haben nicht immer **global** eine Stammfunktion, sondern unter welcher hinreichenden Bedingung auch global?). Es gelten folgende Implikationen im **Reellen** für Funktionen auf kompakten Intervallen:

f Potenzreihe entwickelbar $\Rightarrow f$ ∞ -oft differenzierbar $\Rightarrow f$ differenzierbar $\Rightarrow f$ stetig $\Rightarrow f$ integrierbar $\Rightarrow f$ beschränkt.

Zeige, daß diese Pfeile an keiner Stelle umgedreht werden können (durch Gegenbeispiele).

Dagegen gilt im **Komplexen** für Funktionen auf Gebieten G :

f lokal in eine Potenzreihe entwickelbar $\iff f$ komplex differenzierbar $\iff f$ besitzt lokal eine Stammfunktion \iff das Kurvenintegral ist lokal wegunabhängig (d.h. zu jedem $z_0 \in G$ gibt es ein $U(z_0)$, so daß das Integral über alle in $U(z_0)$ verlaufenden Kurven wegunabhängig ist).

II – ALGEBRA

1. Ringe

Def. Ideal, Hauptideal, maximales Ideal, Primideal. Maximal \Rightarrow prim (denn p maximal $\iff R/p$ Körper $\Rightarrow R/p$ Integritätsring $\iff p$ prim). Konstruktion des Quotientenkörpers von Integritätsringen (wichtig: Bei der Def. der Addition etc. ist eine Wohldefiniertheit zu zeigen!). Def.

euklidischer Ring, Hauptidealring. Wichtige Beispiele: \mathbb{Z} und $K[X]$ für **Körper** K (wie sieht die Abb. $d : R - \{0\} \rightarrow \mathbb{Z}$ hierbei aus?). Def. Primelement, irreduzibles Element. Es gilt: p prim $\iff (p)$ Primideal; p irreduzibel $\iff (p)$ maximal unter allen Hauptidealen. Prim \implies irreduzibel, wieso gilt in Hauptidealringen auch " \Leftarrow "? Def. faktorieller Ring auf 2 Arten mit "irreduzibel" bzw. "prim" (bei "prim" braucht man nicht "eindeutig bis auf Reihenfolge und Einheiten" zu fordern! Weshalb?). Satz: R euklidisch $\implies R$ Hauptidealring $\implies R$ faktoriell (Beweisideen!). Nirgends gilt " \Leftarrow " (für die letzte " \Leftarrow " sollte man das Gegenbeispiel $\mathbb{Z}[X]$ ausführen können: Weshalb faktoriell? Ist (X) darin ein Primideal? (Beachte: $k[X, Y]/(X) \simeq k[Y]$!) Eisenstein. Wie wendet man Eisenstein über \mathbb{Q} an? (Beachte: \mathbb{Q} hat keine Primelemente.) Dabei wird benutzt: Ist R faktoriell, so ist $f \in R[X]$ irreduzibel $\iff f$ primitiv und irreduzibel über $\mathbb{Q}(R)$. Weshalb ist $2x^2 - 6$ irreduzibel über \mathbb{Q} , aber nicht über \mathbb{Z} ?

Weshalb ist \mathbb{Z} faktoriell? Was sind die Primideale und die maximalen Ideale von \mathbb{Z} ? (Beachte: (0) ist prim!) Für welche n ist $\mathbb{Z}/n\mathbb{Z}$ Körper? (Begründung!). Was sind die Einheiten von $\mathbb{Z}/n\mathbb{Z}$? (Begründung: Ist $(m, n) = 1$, so gibt es x, y mit $mx + ny = 1$, also \bar{m} Einheit in $\mathbb{Z}/n\mathbb{Z}$.) Damit zeige: $|\mathbb{Z}/n\mathbb{Z}^*| = \varphi(n)$. Def. von $\varphi(n)$? Für $(n, m) = 1$ gilt $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$ (Umformulierung des Chinesischen Restsatzes!), also $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/nm\mathbb{Z})^*$ und damit $\varphi(n)\varphi(m) = \varphi(mn)$. Da $\varphi(p^k) = p^k - p^{k-1}$ ist (ergibt sich durch Abzählen!), folgt $\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i-1})$, und dies ist trivialerweise $= n \prod (1 - 1/p_i)$.

3. Gruppen

Def. Gruppe, Untergruppe, Normalteiler. Für **Normalteiler** N (und nur für diese!) kann auf der Menge G/N (was ist das?) eine Multiplikation erklärt werden durch $aN \cdot bN = abN$ (wohldefiniert! Warum?). Homomorphiesatz mit Beweisidee (wichtig dabei: $\text{Ker}\varphi$ ist Normalteiler! Definition des Isomorphismus $\psi : G/\text{Ker}\varphi \rightarrow H : \psi(a + \text{Ker}\varphi) := \varphi(a)$. Weshalb wohldefiniert?). Satz von Lagrange (Beweisidee!). Weshalb folgt aus $\text{ord}G = p$, daß G zyklisch ist? Def. zyklisch (beachte: "Von einem Element erzeugt" ist in Gruppentheorie etwas anderes als in Ringtheorie!). Zyklische Gruppen sind $\simeq \mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ (weshalb? Homomorphiesatz! Dabei ist $\text{Ker}\varphi$ zunächst nur **Untergruppe** von \mathbb{Z} . Da aber in \mathbb{Z} Multiplikation eine wiederholte Addition ist, ist jede Untergruppe von \mathbb{Z} auch Ideal, also von der Form $n\mathbb{Z}$). Def. abelsch. Hauptsatz über abelsche Gruppen: $G \simeq \prod (\mathbb{Z}/n_i\mathbb{Z})$ (nur dann eindeutig, wenn die n_i Primzahlpotenzen sind!). Def. auflösbar über Normalteilerkette bzw. über $K^i(G) = \{e\}$. (Beachte: $K(G)$ ist die von allen Kommutatoren **erzeugte** Untergruppe!) Es gilt zyklisch \implies abelsch \implies auflösbar (weshalb?), und nirgends gilt " \Leftarrow " (Gegenbeispiele $\mathbb{Z}_2 \times \mathbb{Z}_2$ bzw. S_3, S_4). Die A_5 ist kleinste nichtauflösbare Gruppe (dazu genaue Def. S_n, A_n , gerade Permutation). Def. p -Gruppe. p -Gruppen sind auflösbar. [Beweisidee: Das Zentrum Z (was ist das?) ist nichttrivial, also ist $\text{ord}(G/Z) < \text{ord}G$. Somit nach Induktion G/Z auflösbar. Trivial ist Z auflösbar (weshalb?). Dann ist auch G auflösbar.] Def. p -Sylowgruppe. Die 3 Sylowsätze. (Beachte: Falls p Sylowgruppe als maximale p -Gruppe definiert wird, ist die Aussage "es gibt p Sylowgruppen" trivial! Außerdem ist die Umkehrung des 2. Sylowsatzes "das Konjugierte einer p -Sylowgruppe ist wieder eine solche", trivial, da Konjugieren ein "innerer Automorphismus" ist!). Es gibt genau eine Sylowgruppe \iff Diese ist Normalteiler (weshalb?).

3. Allgemeine Körpertheorie

Definition Charakteristik eines Körpers. Körpererweiterungen: Wie konstruiert man zu einem irreduziblen Polynom $P \in k[X]$ einen Oberkörper K , so daß P eine Nullstelle in K hat? [Antwort: Bilde $K := k[X]/(P)$. K ist Körper (weshalb?) und enthält k (weshalb?). Dann ist \bar{X} eine Nullstelle von P in K . Def. Zerfällungskörper.

Def. Körpergrad $[K : k]$ (Wieso ist K ein k -Vektorraum?), Folgerung: Ein endlicher Körper K hat p^n Elemente (denn K enthält den Primkörper $k = \mathbb{Z}/p\mathbb{Z}$; K ist also nach Linearer Algebra als Vektorraum $\cong k^n$). Umgekehrt gibt es zu $q = p^n$ stets einen Körper (genannt \mathbb{F}_q) mit q Elementen (nämlich den Zerfällungskörper von $X^q - X$ über $\mathbb{Z}/p\mathbb{Z}$). Beachte $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, aber $\mathbb{F}_{p^2} \not\cong \mathbb{Z}/p^2\mathbb{Z}$ (weshalb?). Gradsatz (Beweisidee!). Def. algebraische Körpererweiterung. $[K : k] < \infty \implies$ algebraisch (Beweis! Beachte dabei, daß "algebraisch" für ein beliebiges $a \in K$ gezeigt werden muß!) Gilt auch

“ \Leftarrow ”? (Gegenbeispiel $K = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots]$.) Aber bei endlich **erzeugten** Körpererweiterungen $K = k(a_1, \dots, a_n)$ gilt “ \Leftrightarrow ” und außerdem \Leftrightarrow “jedes a_i ist algebraisch”. [Beweis: Induktion nach n mit Gradsatz. Induktionsanfang: Zeige zunächst $k(a) = k[a]$ (dies gilt wegen $k[a] \simeq k[X]/(\text{mipo})$, und letzteres ist Körper; weshalb?). Weiter zeige, daß a^0, \dots, a^{m-1} Basis von $k[a]$ über k ist. Damit folgt $[k(a) : k] = \text{gradMipo}$. Weshalb Summe, Produkt algebraischer Zahlen wieder algebraisch? Weshalb ist “algebraisch” ein transitiver Begriff? (Wieso also sind die Nullstellen von $x^4 - \sqrt[3]{2}x - 1$ algebraische Zahlen?).

Def. Konstruierbarkeit mit Zirkel und Lineal. Weshalb bilden konstruierbare Zahlen **Teilkörper** von \mathbb{C} (Polarkoordinatendarstellung!) Satz: x konstruierbar \Leftrightarrow Es gibt Körperkette $\mathbb{Q} \subset K_0 \subset K_1 \subset \dots \subset K_n$ mit $x \in K_n$. [Beweisidee: Für “ \Rightarrow ” muß man die Kreisgleichung und Geradengleichung kennen. Für “ \Leftarrow ” zeigt Polarkoordinatendarstellung, daß man geometrisch \sqrt{z} konstruieren kann.] Folgerung mit Gradsatz: x konstruierbar $\Rightarrow [Q(x) : \mathbb{Q}] = 2^m$. Damit läßt sich **ohne** Galoistheorie zeigen: Würfelverdopplung, Winkeldreiteilung, Kreisquadratur ($[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty!$) unmöglich! Ebenso folgt “ \Rightarrow ” bei der Aussage “ n -Eck konstruierbar $\Leftrightarrow \varphi(n) = 2^m$ ” (Beweis? Für “ \Leftarrow ” wird Galoistheorie gebraucht, Beweisidee!). Mittels Formel für $\varphi(n)$ sind beide Aussagen äquivalent zu $n = 2^k \prod p_i$, wobei p_i **verschiedene** Fermatsche Primzahlen sind.

4. Galoistheorie

Def. von $K : k$ normal: Jedes **irreduzible** Polynom $f \in k[X]$, das in K eine Nullstelle hat, zerfällt in $K[X]$. Beispiel einer nichtnormalen Körpererweiterung. Ist “normal” ein transitiver Begriff? [Gegenbeispiel $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$]. Satz: Ist $K =$ Zerfällungskörper von endlich vielen Polynomen aus $k[X]$, so ist $K : k$ normal. Def. separable Körpererweiterung. Satz: Ein Element $x \in K$ ist separabel über k genau dann, wenn für das zugehörige Minimalpolynom $f \in k[X]$ schon $f' \neq 0$ Nullpolynom ist. Also: In Charakteristik Null ist alles separabel! Evtl. Beispiel einer nichtseparablen Körpererweiterung wissen. Def. vollkommener Körper. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ und alle endlichen Körper sind vollkommen! Satz vom primitiven Element wissen. Def. der Galoisgruppe $\text{Aut } K/k$ (das ist die Gruppe der Automorphismen, die k festlassen). Def. $K : k$ galoissch (zu jedem $x \in K - k$ existiert $\varphi \in \text{Aut } K/k$ mit $\varphi(x) \neq x$). Äquivalent ist “ $K : k$ ist normal und separabel”. Hauptsatz der Galoistheorie: Wie wird die bijektive Abbildung zwischen Untergruppen H und den Zwischenkörpern L konstruiert? (Dazu genaue Def. von $\text{Gal}(K/L)$ und $\text{Fix } H$.) Damit z.B. zeigen können, daß dann nur endlich viele solcher Zwischenkörper existieren. Weitere Anwendungen z.B. wie algebraischer Beweis des Fundamentalsatzes der Algebra, oder aber, wann das regelmäßige n -Eck konstruierbar ist (Beweisideen!) Wissen, daß eine Gleichung n . Grades durch Radikale auflösbar (was heißt das überhaupt?) ist \Leftrightarrow Die Galoisgruppe ist auflösbar (somit ist im allgemeinen eine Gleichung 5. Grades nicht auflösbar, da im allgemeinen Fall die Galoisgruppe $\cong S_5$ ist und die S_5 nicht auflösbar ist.

III – FACHDIDAKTIK

Def. von \mathbb{N} durch die Peano-Axiome. Konstruktion von \mathbb{Q} aus \mathbb{Z} (siehe Abschnitt “Ringe”). Konstruktion von \mathbb{R} aus \mathbb{Q} , indem man die Menge aller Cauchyfolgen (a_n) nimmt mit $a_n \in \mathbb{Q}$ und zwei Cauchyfolgen (a_n) und (a'_n) in dieselbe Klasse einordnet, wenn $(a_n - a'_n)$ eine Nullfolge ist. Weshalb ist man nicht mit \mathbb{Q} zufrieden? (Antwort: Weil in \mathbb{Q} nicht jede Cauchyfolge konvergiert, beschränkte Mengen kein Supremum haben, das Majorantenkriterium für unendliche Reihe nicht gilt usw.) (Dies mache man sich an Gegenbeispielen klar!)

Def. der Potenzen entweder über $a^{p/q} := \sqrt[q]{a^p}$ und $a^x = \lim a^{x_n}$, wenn $x_n \in \mathbb{Q}$ und $x_n \rightarrow x$ geht. (Dabei zeige Wohldefiniertheit!) Oder es kann a^x über $\exp(x \log a)$ definiert werden. Weshalb stimmen beide Definitionen überein? Weshalb stimmt der geometrisch definierte \sin mit der Potenzreihe überein? (Antwort: Geometrischen \sin differenzieren, dann Taylorformel!)

IV – ZAHLENTHEORIE

Fundamentalsatz (Beweis nach Zermelo und/oder über “ \mathbb{Z} euklidisch” \Rightarrow “ \mathbb{Z} faktoriell”). Beachte, daß “ p Primzahl” zunächst bedeutet “ p irreduzibel”; daß dann auch “ p Primelement” i.S.d. Algebra ist, muß gezeigt werden! Satz von Euklid (Beweis). Primzahlsatz $\pi(x) \approx x/\log x$ kennen. Mersennesche und Fermatsche Primzahlen (weshalb ist bei $p = 2^q - 1$ schon $q \in \mathbb{P}$ bzw. bei $p = 2^n + 1$ schon $n = 2^k$?) Def. $d = \text{ggT}(a, b)$ durch Teilbarkeitseigenschaft (dabei ist Existenz nicht klar!). Die Existenz folgt aus den äquivalenten Darstellungen $d = \prod p_i^{\min(n_i, m_i)}$ [hier wird \mathbb{Z} faktoriell benutzt!] bzw. $(d) = (a) + (b)$ [hier wird \mathbb{Z} Hauptidealring benutzt! Def. von $(a) + (b)$?] bzw. $d =$ kleinste positive Zahl der Form $ax + by$ (hier wird euklidischer Algorithmus benutzt!). Beweisideen für diese Äquivalenzen? Wie berechnet man ggT am besten?

Def. und Rechenregeln für Kongruenzen. Chinesischer Restsatz (auch anwenden können, wenn die Moduln nicht teilerfremd sind). Def. Primitivwurzel mod n . Satz: Ist n ungerade Primpotenz, so existiert Primitivwurzel (algebraisch heißt dies: $(\mathbb{Z}/n\mathbb{Z})^*$ ist zyklisch!) Dann gibt es $\varphi(\varphi(n))$ viele Primitivwurzeln mod n . Def. φ -Funktion und Eigenschaften (s. Abschnitt “Ringe”). Satz von Euler-Fermat. [Beweis! Ein algebraischer Beweis kann so aussehen: Sei $G = (\mathbb{Z}/n\mathbb{Z})^*$. Dann ist $\text{ord}G = \varphi(n)$. Andererseits gilt stets $a^{\text{ord}G} = e$ (folgt aus Lagrange!). Damit $a^{\varphi(n)} \equiv 1 \pmod{n}$.] Satz von Wilson (Beweis!). Def. quadratischer Rest, Legendresymbol. Warum gibt es $(p-1)/2$ Reste? (Antwort: Die Zahlen $1^2, 2^2, \dots, (p-2)^2, (p-1)^2$ sind mod p genau die quadratischen Reste, und es gilt $x^2 \equiv y^2 \pmod{p} \iff x \equiv \pm y \pmod{p}$.) Eulersches Kriterium (ist Verallgemeinerung des “kleinen Fermat”!) Gaußsches Reziprozitätsgesetz mit Ergänzungssätzen (Beispiele!). Der Ring $\mathbb{Z}[i]$ (Euklidisch. Einheiten? Wann ist für Primzahlen p das Ideal $p\mathbb{Z}[i]$ prim? Wann ist $p = a^2 + b^2$?)